10/026,640
#4

# 日 本 国 特 許 庁
# JAPAN PATENT OFFICE



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年１２月２８日

出願番号
Application Number: 特願２０００－４０２９５９

[ST.10/C]: [ＪＰ２０００－４０２９５９]

出願人
Applicant(s): 株式会社エヌ・ティ・ティ・ドコモ





２００２年 ２月１５日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号 出証特２００２－３００７７８０

Docket No. 217759US2/sbj

#4

# IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Takashi SUZUKI, et al.

SERIAL NO: 10/026,640

FILED: December 27, 2001

GAU: 2131

EXAMINER:

FOR: CONTENT DISTRIBUTION SYSTEM, COPYRIGHT PROTECTION SYSTEM AND CONTENT RECEIVING TERMINAL

## REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number [US App No], filed [US App Dt], is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date of U.S. Provisional Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §119(e)**.

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

| COUNTRY | APPLICATION NUMBER | MONTH/DAY/YEAR |
|---|---|---|
| JAPAN | 2000-402959 | December 28, 2000 |

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number .
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

(B) Application Serial No.(s)

☐ are submitted herewith

☐ will be submitted prior to payment of the Final Fee



Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Joseph A. Scafetta Jr.

Marvin J. Spivak
Registration No. 24,913

Joseph A. Scafetta, Jr.
Registration No. 26,803

22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)

【書類名】　特許願
【整理番号】　ND12-0338
【提出日】　平成12年12月28日
【あて先】　特許庁長官　及川　耕造　殿
【国際特許分類】　H04L 12/00
【発明者】
【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内
【氏名】　鈴木　敬
【発明者】
【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内
【氏名】　河原　敏朗
【発明者】
【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内
【氏名】　栄藤　稔
【特許出願人】
【識別番号】　392026693
【氏名又は名称】　株式会社エヌ・ティ・ティ・ドコモ
【代理人】
【識別番号】　100070150
【弁理士】
【氏名又は名称】　伊東　忠彦
【手数料の表示】
【予納台帳番号】　002989
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　コンテンツ配信システム、著作権保護システム及びコンテンツ受信端末

【特許請求の範囲】

【請求項１】　コンテンツを保有し配信する１つ以上のコンテンツ配信サーバと、該コンテンツの著作権を保護する著作権保護システムと、該コンテンツ配信サーバからのコンテンツを受信するコンテンツ受信端末とを有するコンテンツ配信システムにおいて、

著作権保護システムは、

コンテンツの所在を示すコンテンツ所在情報を暗号化する暗号化手段と、

前記暗号化されたコンテンツ所在情報を含んだコンテンツ選択文書を生成するコンテンツ選択文書生成手段と、

前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ選択文書送信手段と、

を備え、

コンテンツ受信端末は、

著作権保護システムからのコンテンツ選択文書を受信するコンテンツ選択文書受信手段と、

前記受信したコンテンツ選択文書から暗号化されたコンテンツ所在情報を抽出するコンテンツ所在情報抽出手段と、

前記抽出した暗号化されたコンテンツ所在情報を復号する復号手段と、

前記復号したコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、

前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信するコンテンツ受信手段と、

を備えるコンテンツ配信システム。

【請求項２】　コンテンツを保有し配信する１つ以上のコンテンツ配信サーバと、該コンテンツの著作権を保護する著作権保護システムと、該コンテンツ配信サーバからのコンテンツを受信するコンテンツ受信端末とを有するコンテンツ

配信システムにおいて、

著作権保護システムは、

コンテンツの所在を示すコンテンツ所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を生成するコンテンツ選択文書生成手段と、

前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ選択文書送信手段と、

を備え、

コンテンツ受信端末は、

著作権保護システムからのコンテンツ選択文書を受信するコンテンツ選択文書受信手段と、

前記受信したコンテンツ選択文書からコンテンツ選択文書と、所在認証情報とを抽出する情報抽出手段と、

前記抽出した所在認証情報に基づいて、コンテンツの所在の正当性を検証する正当性検証手段と、

前記検証によりコンテンツの所在の正当性が確認された場合に、前記抽出したコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、

前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信するコンテンツ受信手段と、

を備えるコンテンツ配信システム。

【請求項３】　コンテンツを保有し配信する１つ以上のコンテンツ配信サーバと、該コンテンツの著作権を保護する著作権保護システムと、該コンテンツ配信サーバからのコンテンツを受信するコンテンツ受信端末とを有するコンテンツ配信システムにおいて、

著作権保護システムは、

コンテンツの所在を示すコンテンツ所在情報を暗号化する暗号化手段と、

前記暗号化されたコンテンツ所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を生成するコンテンツ選択文書生

成手段と、

前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ選択文書送信手段と、

を備え、

コンテンツ受信端末は、

著作権保護システムからのコンテンツ選択文書を受信するコンテンツ選択文書受信手段と、

前記受信したコンテンツ選択文書から暗号化されたコンテンツ所在情報と、所在認証情報とを抽出する情報抽出手段と、

前記抽出した暗号化されたコンテンツ所在情報を復号する復号手段と、

前記抽出した所在認証情報に基づいて、コンテンツの所在の正当性を検証する正当性検証手段と、

前記検証によりコンテンツの所在の正当性が確認された場合に、前記復号したコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、

前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信するコンテンツ受信手段と、

を備えるコンテンツ配信システム。

【請求項４】　請求項３に記載のコンテンツ配信システムにおいて、

前記暗号化手段は、前記コンテンツ所在情報と前記所在認証情報とをまとめて暗号化し、

前記コンテンツ選択文書生成手段は、前記暗号化データを含んだコンテンツ選択文書を生成し、

前記情報抽出手段は、前記受信したコンテンツ選択文書から暗号化データを抽出し、

前記復号手段は、前記抽出した暗号化データからコンテンツ所在情報と所在認証情報とを復号し、

前記正当性検証手段は、前記復号した所在認証情報に基づいて、コンテンツの所在の正当性を検証するようにしたコンテンツ配信システム。

【請求項５】　コンテンツの著作権を保護する著作権保護システムにおいて、

コンテンツの所在を示すコンテンツ所在情報を暗号化する暗号化手段と、

前記暗号化されたコンテンツ所在情報を含んだコンテンツ選択文書を生成するコンテンツ選択文書生成手段と、

前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ選択文書送信手段と、

を備える著作権保護システム。

【請求項６】　コンテンツの著作権を保護する著作権保護システムにおいて、

コンテンツの所在を示すコンテンツ所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を生成するコンテンツ選択文書生成手段と、

前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ選択文書送信手段と、

を備える著作権保護システム。

【請求項７】　コンテンツの著作権を保護する著作権保護システムにおいて、

コンテンツの所在を示す所在情報を暗号化する暗号化手段と、

前記暗号化された所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を生成するコンテンツ選択文書生成手段と、

前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ選択文書送信手段と、

を備える著作権保護システム。

【請求項８】　請求項７に記載の著作権保護システムにおいて、

前記暗号化手段は、前記コンテンツ所在情報と前記所在認証情報とをまとめて暗号化し、

前記コンテンツ選択文書生成手段は、前記暗号化データを含んだコンテンツ選択文書を生成するようにした著作権保護システム。

【請求項９】　請求項５、７又は８に記載の著作権保護システムにおいて、

コンテンツ所在情報を含むコンテンツ情報、該コンテンツ情報に関連したアクセス情報及びコンテンツを利用するユーザ又はコンテンツ受信端末の正当性を証明するユーザ認証情報を取得する情報取得手段と、

前記取得したアクセス情報とユーザ認証情報に基づいてコンテンツ所在情報の暗号化方式を選択する暗号化方式選択手段と、

を備え、

前記暗号化手段は、前記選択された暗号化方式を用いてコンテンツ所在情報を暗号化するようにした著作権保護システム。

【請求項１０】　請求項６、７又は８に記載の著作権保護システムにおいて、

コンテンツ所在情報を含むコンテンツ情報、該コンテンツ情報に関連したアクセス情報及びコンテンツ所在情報で指定されるコンテンツの所在の正当性を証明する所在認証情報を取得する情報取得手段を備え、

コンテンツ選択文書生成手段は、前記取得された所在認証情報を含んだコンテンツ選択文書を生成するようにした著作権保護システム。

【請求項１１】　請求項５、７乃至１０の何れかに記載の著作権保護システムにおいて、

前記暗号化されたコンテンツ所在情報を復号する鍵をコンテンツ受信端末と共有する鍵共有手段と、

前記鍵が共有された後にコンテンツ所在情報で指定されるコンテンツの利用料金を課金する課金手段と、

を備える著作権保護システム。

【請求項１２】　暗号化されたコンテンツ所在情報を含んだコンテンツ選択文書を受信するコンテンツ選択文書受信手段と、

前記受信したコンテンツ選択文書からコンテンツ所在情報を抽出するコンテンツ所在情報抽出手段と、

前記抽出した暗号化されたコンテンツ所在情報を復号する復号手段と、

前記復号したコンテンツ所在情報で指定されるコンテンツを保有するコンテン

ツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、

前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信するコンテンツ受信手段と、

を備えるコンテンツ受信端末。

【請求項１３】　コンテンツの所在を示すコンテンツ所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を受信するコンテンツ選択文書受信手段と、

前記受信したコンテンツ選択文書からコンテンツ所在情報と、所在認証情報とを抽出する情報抽出手段と、

前記抽出した所在認証情報に基づいて、コンテンツの所在の正当性を検証する正当性検証手段と、

前記検証によりコンテンツの所在の正当性が確認された場合に、前記抽出したコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、

前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信するコンテンツ受信手段と、

を備えるコンテンツ受信端末。

【請求項１４】　暗号化されたコンテンツの所在を示すコンテンツ所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を受信するコンテンツ選択文書受信手段と、

前記受信したコンテンツ選択文書から暗号化されたコンテンツ所在情報と、所在認証情報とを抽出する情報抽出手段と、

前記抽出した暗号化されたコンテンツ所在情報を復号する復号手段と、

前記抽出した所在認証情報に基づいて、コンテンツの所在の正当性を検証する正当性検証手段と、

前記検証によりコンテンツの所在の正当性が確認された場合に、前記復号したコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、

前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信

するコンテンツ受信手段と、

を備えるコンテンツ受信端末。

【請求項１５】　請求項１４に記載のコンテンツ受信端末において、

前記情報抽出手段は、前記受信したコンテンツ選択文書から暗号化データを抽出し、

前記復号手段は、前記抽出した暗号化データからコンテンツ所在情報と所在認証情報とを復号し、

前記正当性検証手段は、前記復号した所在認証情報に基づいて、コンテンツの所在の正当性を検証するようにしたコンテンツ受信端末。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、著作物であるコンテンツの著作権を保護するためのシステムに関し、特に、著作物であるコンテンツを配信するコンテンツ配信システムにおける著作物保護技術に関する。

【０００２】

【従来の技術】

近年、高速なアクセス回線の普及やインターネット技術の発展に伴い、映像や音楽等のコンテンツをインターネット経由で配信するコンテンツ配信サービスが実現されている。このようなコンテンツ配信サービスを普及させるためには、著作物であるコンテンツの所有者に対して適正な対価が支払われることが不可欠である。このため、コンテンツの利用者に対し課金を行うシステムが必要となる。

【０００３】

コンテンツの利用量に応じて利用者に対し課金するコンテンツ配信システムには、例えば公開特許公報「特開２０００－１０１５７３」に開示されたシステムがある。この「特開２０００－１０１５７３」に開示されたコンテンツ配信システムでは、サーバがコンテンツ受信端末の要求に応じてコンテンツの配信処理を行うとともに、サーバにおいてコンテンツ利用に対する課金処理を行っている。

【０００４】

【発明が解決しようとする課題】

ところで、サービス利用者が多い大規模なコンテンツ配信システムでは、ユーザ認証及び課金処理とコンテンツの配信処理とを同一のサーバで行うと、ユーザ認証及び課金処理の負担が大きいため、同時に配信可能なユーザ数が減少する等の問題が生じる。従って、サーバの負荷分散のため、ユーザ認証及び課金処理とコンテンツの配信処理とを異なるサーバで分散する必要が生じる。また、このような負荷分散を図ることで、コンテンツ保有者とコンテンツ利用に対する課金業者とを別々にすることができ、より多様なコンテンツ配信サービスが可能になるという効果もある。

【０００５】

このように負荷分散を図ったコンテンツ配信システムとしては、例えば図８に示すような構成が考えられる。図８において、認証･課金サーバ２００は、コンテンツへのリンク情報が含まれるコンテンツ選択文書２０１を蓄積している。コンテンツ選択文書２０１は、例えばＨＴＭＬ形式の文書であり、リンク情報で示されるコンテンツが有料の場合には文書全体が暗号化され、無料の場合には暗号化されずに、コンテンツ受信端末１００へ送信される。

【０００６】

このため、上述の「特開２０００－１０１５７３」に開示されたコンテンツ配信システムにおいて、認証・課金サーバとコンテンツ配信サーバとを分離した場合、個々のコンテンツに対し課金を行うためには、コンテンツの課金種別毎にコンテンツ選択文書を用意する必要がある。即ち、無料コンテンツを希望するユーザには、暗号化されていない無料コンテンツの選択文書を配布し、有料コンテンツについても希望するユーザには、暗号化されていない無料コンテンツの選択文書と暗号化された有料コンテンツの選択文書の双方を配布する必要があり、効率的ではなかった。

【０００７】

また、「特開２０００－１０１５７３」に開示されたコンテンツ配信システムでは、認証・課金サーバとコンテンツ配信サーバとを分離した場合、コンテンツ配信サーバに対する認証機構を備えていないことが問題となり得る。例えば、不

正なコンテンツサーバを示すリンク情報がコンテンツ選択文書に埋め込まれた場合、コンテンツ受信端末は、その不正なサーバへコンテンツ配信を要求することになり、違法コピーされたコンテンツが配信され、適切な課金が困難になる等の問題が生じ得る。

【０００８】

本発明は、上記問題点を解決するものであり、その目的は、大規模なシステムを構築可能であるとともに、コンテンツ課金を適正に行うことができるコンテンツ配信システム、著作権保護システム及びコンテンツ受信端末を提供することにある。

【０００９】

【課題を解決するための手段】

上記の目的を達成するため、本発明は請求項１に記載されるように、コンテンツを保有し配信する１つ以上のコンテンツ配信サーバと、該コンテンツの著作権を保護する著作権保護システムと、該コンテンツ配信サーバからのコンテンツを受信するコンテンツ受信端末とを有するコンテンツ配信システムにおいて、著作権保護システムは、コンテンツの所在を示すコンテンツ所在情報を暗号化する暗号化手段と、前記暗号化されたコンテンツ所在情報を含んだコンテンツ選択文書を生成するコンテンツ選択文書生成手段と、前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ選択文書送信手段とを備え、コンテンツ受信端末は、著作権保護システムからのコンテンツ選択文書を受信するコンテンツ選択文書受信手段と、前記受信したコンテンツ選択文書から暗号化されたコンテンツ所在情報を抽出するコンテンツ所在情報抽出手段と、前記抽出した暗号化されたコンテンツ所在情報を復号する復号手段と、前記復号したコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信するコンテンツ受信手段とを備える。

【００１０】

このように、コンテンツ配信サーバと著作権保護システムが分離され、且つ、

コンテンツの配信に際してコンテンツ配信サーバと著作権保護システムとの間で情報のやり取りが行われることがないため、コンテンツ配信サーバの負荷を軽減させて、大規模なコンテンツ配信システムを構築することができる。

【００１１】

また、従来のようにコンテンツ選択文書全体が暗号化されるのではなく、コンテンツ所在情報だけを選択的に暗号化することが可能であるため、例えば課金種別に応じて暗号化された複数のコンテンツ所在情報をコンテンツ選択文書に含ませておくことで、効率的なコンテンツ課金を行うことができる。

【００１２】

また、本発明は請求項２に記載されるように、コンテンツを保有し配信する１つ以上のコンテンツ配信サーバと、該コンテンツの著作権を保護する著作権保護システムと、該コンテンツ配信サーバからのコンテンツを受信するコンテンツ受信端末とを有するコンテンツ配信システムにおいて、著作権保護システムは、コンテンツの所在を示すコンテンツ所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を生成するコンテンツ選択文書生成手段と、前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ選択文書送信手段とを備え、コンテンツ受信端末は、著作権保護システムからのコンテンツ選択文書を受信するコンテンツ選択文書受信手段と、前記受信したコンテンツ選択文書からコンテンツ選択文書と、所在認証情報とを抽出する情報抽出手段と、前記抽出した所在認証情報に基づいて、コンテンツの所在の正当性を検証する正当性検証手段と、前記検証によりコンテンツの所在の正当性が確認された場合に、前記抽出したコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信するコンテンツ受信手段とを備える。

【００１３】

このように、コンテンツ配信サーバと著作権保護システムが分離され、且つ、コンテンツの配信に際してコンテンツ配信サーバと著作権保護システムとの間で情報のやり取りが行われることがないため、コンテンツ配信サーバの負荷を軽減

させて、大規模なコンテンツ配信システムを構築することができる。また、著作権保護システムからコンテンツ受信端末へコンテンツ所在情報とコンテンツの所在の正当性を証明する所在認証情報とが送信されるため、コンテンツ受信端末は、コンテンツ所在情報で示されるコンテンツの所在の正当性を検証することができ、不正なサーバへアクセスして配信を受けることが防止され適切な課金処理を行うことができる。

【００１４】

また、本発明は請求項３に記載されるように、コンテンツを保有し配信する１つ以上のコンテンツ配信サーバと、該コンテンツの著作権を保護する著作権保護システムと、該コンテンツ配信サーバからのコンテンツを受信するコンテンツ受信端末とを有するコンテンツ配信システムにおいて、著作権保護システムは、コンテンツの所在を示すコンテンツ所在情報を暗号化する暗号化手段と、前記暗号化されたコンテンツ所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を生成するコンテンツ選択文書生成手段と、前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ選択文書送信手段とを備え、コンテンツ受信端末は、著作権保護システムからのコンテンツ選択文書を受信するコンテンツ選択文書受信手段と、前記受信したコンテンツ選択文書から暗号化されたコンテンツ所在情報と、所在認証情報とを抽出する情報抽出手段と、前記抽出した暗号化されたコンテンツ所在情報を復号する復号手段と、前記抽出した所在認証情報に基づいて、コンテンツの所在の正当性を検証する正当性検証手段と、前記検証によりコンテンツの所在の正当性が確認された場合に、前記復号したコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信するコンテンツ受信手段とを備える。

【００１５】

この場合には、請求項１及び２に記載された発明と同様、コンテンツ配信サーバと著作権保護システムが分離され、且つ、コンテンツの配信に際してコンテンツ配信サーバと著作権保護システムとの間で情報のやり取りが行われることがな

いため、コンテンツ配信サーバの負荷を軽減させて、大規模なコンテンツ配信システムを構築することができる。

【００１６】

また、請求項１に記載された発明と同様、コンテンツ選択文書全体が暗号化されるのではなく、コンテンツ所在情報だけを選択的に暗号化することが可能であるため、例えば課金種別に応じて暗号化された複数のコンテンツ所在情報をコンテンツ選択文書に含ませておくことで、効率的なコンテンツ課金を行うことができる。

【００１７】

また、請求項２に記載された発明と同様、著作権保護システムからコンテンツ受信端末へコンテンツの所在の正当性を証明する所在認証情報が送信されるため、コンテンツ受信端末は、コンテンツ所在情報で示されるコンテンツの所在の正当性を検証することができ、不正なサーバへアクセスして配信を受けることが防止され適切な課金処理を行うことができる。

【００１８】

この場合、請求項４に記載されるように、前記コンテンツ配信システムにおいて、前記暗号化手段は、前記コンテンツ所在情報と前記所在認証情報とをまとめて暗号化し、前記コンテンツ選択文書生成手段は、前記暗号化データを含んだコンテンツ選択文書を生成し、前記情報抽出手段は、前記受信したコンテンツ選択文書から暗号化データを抽出し、前記復号手段は、前記抽出した暗号化データからコンテンツ所在情報と所在認証情報とを復号し、前記正当性検証手段は、前記復号した所在認証情報に基づいて、コンテンツの所在の正当性を検証することができる。

【００１９】

また、請求項５乃至１１に記載された著作権保護システムは、上述した請求項１乃至４に記載されたコンテンツ配信システムに適した著作権保護システムである。　具体的には、本発明は請求項５に記載されるように、コンテンツの著作権を保護する著作権保護システムにおいて、コンテンツの所在を示すコンテンツ所在情報を暗号化する暗号化手段と、前記暗号化されたコンテンツ所在情報を含ん

だコンテンツ選択文書を生成するコンテンツ選択文書生成手段と、前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ選択文書送信手段とを備える。

【００２０】

また、本発明は請求項６に記載されるように、コンテンツの著作権を保護する著作権保護システムにおいて、コンテンツの著作権を保護する著作権保護システムにおいて、コンテンツの所在を示すコンテンツ所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を生成するコンテンツ選択文書生成手段と、前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ選択文書送信手段とを備える。

【００２１】

また、本発明は請求項７に記載されるように、コンテンツの著作権を保護する著作権保護システムにおいて、コンテンツの所在を示す所在情報を暗号化する暗号化手段と、前記暗号化された所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を生成するコンテンツ選択文書生成手段と、前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ選択文書送信手段とを備える。

【００２２】

この場合、請求項８に記載されるように、前記著作権保護システムにおいて、前記暗号化手段は、前記暗号化手段は、前記コンテンツ所在情報と前記所在認証情報とをまとめて暗号化し、前記コンテンツ選択文書生成手段は、前記暗号化データを含んだコンテンツ選択文書を生成することができる。

【００２３】

また、本発明は請求項９に記載されるように、請求項５、７又は８に記載の著作権保護システムにおいて、コンテンツ所在情報を含むコンテンツ情報、該コンテンツ情報に関連したアクセス情報及びコンテンツを利用するユーザ又はコンテンツ受信端末の正当性を証明するユーザ認証情報を取得する情報取得手段と、前記取得したアクセス情報とユーザ認証情報に基づいてコンテンツ所在情報の暗号化方式を選択する暗号化方式選択手段とを備え、前記暗号化手段は、前記選択さ

れた暗号化方式を用いてコンテンツ所在情報を暗号化する。

【００２４】

また、本発明は請求項１０に記載されるように、請求項６、７又は８に記載の著作権保護システムにおいて、コンテンツ所在情報を含むコンテンツ情報、該コンテンツ情報に関連したアクセス情報及びコンテンツ所在情報で指定されるコンテンツの所在の正当性を証明する所在認証情報を取得する情報取得手段を備え、コンテンツ選択文書生成手段は、前記取得された所在認証情報を含んだコンテンツ選択文書を生成する。

【００２５】

また、本発明は請求項１１に記載されるように、請求項５、７乃至１０の何れかに記載の著作権保護システムにおいて、前記暗号化されたコンテンツ所在情報を復号する鍵をコンテンツ受信端末と共有する鍵共有手段と、前記鍵が共有された後にコンテンツ所在情報で指定されるコンテンツの利用料金を課金する課金手段とを備える。

【００２６】

また、請求項１２乃至１５に記載されたコンテンツ受信端末は、上述した請求項１乃至４に記載されたコンテンツ配信システムに適したコンテンツ受信端末である。具体的には、本発明のコンテンツ受信端末は請求項１２に記載されるように、暗号化されたコンテンツ所在情報を含んだコンテンツ選択文書を受信するコンテンツ選択文書受信手段と、前記受信したコンテンツ選択文書からコンテンツ所在情報を抽出するコンテンツ所在情報抽出手段と、前記抽出した暗号化されたコンテンツ所在情報を復号する復号手段と、前記復号したコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信するコンテンツ受信手段とを備える。

【００２７】

また、本発明のコンテンツ受信端末は請求項１３に記載されるように、コンテンツの所在を示すコンテンツ所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を受信するコンテンツ選択文書受信

手段と、前記受信したコンテンツ選択文書からコンテンツ所在情報と、所在認証情報とを抽出する情報抽出手段と、前記抽出した所在認証情報に基づいて、コンテンツの所在の正当性を検証する正当性検証手段と、前記検証によりコンテンツの所在の正当性が確認された場合に、前記抽出したコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信するコンテンツ受信手段とを備える。

【００２８】

また、本発明のコンテンツ受信端末は請求項１４に記載されるように、暗号化されたコンテンツの所在を示すコンテンツ所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を受信するコンテンツ選択文書受信手段と、前記受信したコンテンツ選択文書から暗号化されたコンテンツ所在情報と、所在認証情報とを抽出する情報抽出手段と、前記抽出した暗号化されたコンテンツ所在情報を復号する復号手段と、前記抽出した所在認証情報に基づいて、コンテンツの所在の正当性を検証する正当性検証手段と、前記検証によりコンテンツの所在の正当性が確認された場合に、前記復号したコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信するコンテンツ受信手段とを備える。

【００２９】

この場合、請求項１５に記載されるように前記コンテンツ受信端末において、前記情報抽出手段は、前記受信したコンテンツ選択文書から暗号化データを抽出し、前記復号手段は、前記抽出した暗号化データからコンテンツ所在情報と所在認証情報とを復号し、前記正当性検証手段は、前記復号した所在認証情報に基づいて、コンテンツの所在の正当性を検証することができる。

【００３０】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて説明する。図１は、本発明の第１

実施例に係るコンテンツ配信システムの構成例を示す図である。同図に示すコンテンツ配信システム１０００は、コンテンツ受信端末１１００、コンテンツサーバ群１２００、著作権保護システム１３００を備えて構成される。コンテンツ受信端末１１００と、コンテンツサーバ群１２００及び著作権保護システム１３００とは、ネットワーク１５００を介して接続される。

【００３１】

コンテンツ配信システム１０００では、著作権保護システム１３００がオーディオビジュアルデータであるコンテンツの所在を示すコンテンツ所在情報を暗号化して送信しており、この暗号化されたコンテンツ所在情報を受信したコンテンツ受信端末１１００が、復号鍵を保有する場合にのみ、暗号化されたコンテンツ所在情報を復号し、コンテンツサーバ群１２００にアクセスすることでコンテンツの配信を受けることができるようになっている。また、コンテンツ配信システム１０００では、著作権保護システム１３００がコンテンツの所在の正当性を証明する所在認証情報を保有し、これを送信しており、この所在認証情報を取得したコンテンツ受信端末１１００が、コンテンツの所在の正当性を検証することができるようになっている。

【００３２】

著作権保護システム１３００は、コンテンツ選択文書１４００を生成し、コンテンツ受信端末１１００へ送信する機能を有する。図２は、第１実施例に係る著作権保護システム１３００の構成例を示す図である。

【００３３】

コンテンツ受信端末１１００は、コンテンツの配信を受ける際、ユーザの操作により著作権保護システム１３００にアクセスする。このとき端末認証部１３０２は、著作権保護システム１３００にアクセスするコンテンツ受信端末１１００又は該コンテンツ受信端末１１００のユーザの認証を行う。認証にはコンテンツ受信端末１１００又は該コンテンツ受信端末１１００のユーザに付与されたＩＤとパスワードを用いた方法等を利用することができる。

【００３４】

著作権保護システム１３００の内部で生成若しくは外部から入力されたコンテ

ンツ所在情報１３０８には、コンテンツ配信サーバの正当性を証明する所在認証情報１３１１が付与される。この際、所在認証情報であることを示すタグが所在認証情報タグ付加部１３１２により付加される。所在認証情報の発行元には、著作権保護システム１３００、コンテンツ配信サーバ運用者、コンテンツホルダとうが考えられるが、本実施例では著作権保護システム１３００を発行元とする。

【００３５】

また、所在認証情報１３１１の生成や検証には、公開鍵暗号系を適用したデジタル署名等を利用することができる。この場合、コンテンツ所在情報１３０８に一方向性関数を施し、その演算結果を公開鍵暗号方式の秘密鍵を用いて暗号化したものを所在認証情報１３１１とする。コンテンツ所在情報１３０８を検証する場合には、受け取ったコンテンツ所在情報に一方向性関数を施した結果と、受け取った所在認証情報１３１１を秘密鍵に対応する公開鍵で復号した結果とを比較する。そして、これらが一致すれば合格、一致しなければ不合格と判定する。デジタル署名については、辻井、笠原著「暗号と情報セキュリティ」Ｐ１３０～１４７に詳しい。

【００３６】

所在認証情報タグ付加部１３１２は、所在認証情報１３１１に、所在認証情報であることを示すタグ（以下「所在認証情報タグ」と称する）を付加する。情報付加部１３１４は、コンテンツ所在情報１３０８に、所在認証情報タグ付加部１３１２から出力される、所在認証情報１３１１と所在認証情報タグとを付加する。

【００３７】

暗号化部１３０９は、情報付加部１３１４から出力される、所在認証情報１３１１が付加されたコンテンツ所在情報１３０８を、コンテンツの課金種別に対応する暗号化鍵１３０７により暗号化し、この暗号化したコンテンツ所在情報に、コンテンツ所在情報が暗号化されていることを示すタグ（以下「暗号化情報タグ」と称する）を付加する。

【００３８】

コンテンツ所在情報の暗号化には、ＤＥＳやＴＤＥＳなどを適用することがで

きる。また暗号化に用いられる暗号化鍵１３０７は、所在情報暗号化鍵共有部１３０３において、コンテンツ受信端末１１００と共有される。暗号化鍵１３０７の共有には、Ｄｅｆｆｉｅ－Ｈｅｌｌｍａｎ（今井秀樹他著「情報セキュリティ理論」Ｐ１３２～１３５参照）の鍵配送アルゴリズム等を利用することができる。また、所在情報暗号化鍵共有部１３０３は、コンテンツ受信端末１１００との間で共有される暗号化鍵１３０７の共有履歴を記録しており、この共有履歴を課金部１３０６に提供する。

【００３９】

コンテンツ選択文書生成部１３１０は、暗号化されたコンテンツ所在情報１３０８を複数組み合わせてコンテンツ選択文書を生成する。署名部１３１３は、コンテンツ選択文書の送信元となる著作権保護システム１３００の正当性を証明するために、生成されたコンテンツ選択文書に対し著作権保護システム１３００に対応する署名を付加する。コンテンツ選択文書配信部１３０４は、この署名が付加されたコンテンツ選択文書を、上述した端末認証部１３０２によって認証されたコンテンツ受信端末１１００へ配信する。

【００４０】

再び図１に戻って説明する。コンテンツ受信端末１１００へ配信されるコンテンツ選択文書は、例えば同図に示すコンテンツ選択文書１４００の構成を有している。コンテンツ選択文書１４００は、無料コンテンツである音楽データ及びビデオデータに対応するコンテンツ所在情報及び所在認証情報を含んだ情報群１４０１と、有料コンテンツである音楽データ及びビデオデータに対応するコンテンツ所在情報及び所在認証情報を含んだ情報群１４０２と、コンテンツ選択文書１４００の送信元を証明する署名（コンテンツ選択文書署名）１４０４を含んでいる。このコンテンツ選択文書１４００において、無料コンテンツである音楽データ及びビデオデータに対応するコンテンツ所在情報は、不特定多数のコンテンツ受信端末が配信を受けることができるように暗号化されておらず、有料コンテンツである音楽データ及びビデオデータに対応するコンテンツ所在情報のみが暗号化されている。なお、コンテンツ選択文書１４００には、コンテンツ所在情報及び所在認証情報とともに暗号化情報タグ及び所在認証情報タグが含まれるが、図

１ではこれらを省略している。

【００４１】

課金部１３０６は、所在情報暗号化鍵共有部１３０３から提供される鍵共有履歴に基づいて、コンテンツ受信端末１１００へ配信したコンテンツ選択文書内のコンテンツ所在情報を暗号化するために用いた暗号化鍵１３０７を認識し、この鍵１３０７に対応する課金種別に応じて、コンテンツ受信端末１１００のユーザ、即ちコンテンツ利用者に対して課金を行う。コンテンツ利用者の特定に際して課金部１３０６は、端末認証部１３０２から提供されるコンテンツ受信端末１１００又はユーザの識別情報を利用する。識別情報としては端末認証部１３０２による認証の際に用いられるコンテンツ受信端末１１００又は該コンテンツ受信端末１１００のユーザに付与されたＩＤが利用される。

【００４２】

なお、課金部１３０６は、課金に際して、鍵共有履歴を用いる他に、コンテンツサーバ群１２００の各コンテンツ配信サーバがコンテンツ受信端末１１００に対し、コンテンツを配信した履歴を用いることもできる。この場合、アクセス情報受信部１３０１は、コンテンツサーバ群１２００内のコンテンツ配信サーバからの配信履歴を受信する。課金部１３０６は、この受信された配信履歴に基づいてコンテンツ受信端末１１００のユーザに対して課金を行う。

【００４３】

課金部１３０６による課金処理の結果は、課金情報として課金情報蓄積サーバ１３０５に蓄積される。

【００４４】

このように、課金に際して暗号化鍵１３０７の共有履歴とコンテンツの配信履歴とを使い分けることにより、様々な課金形態を実現することができる。例えば、暗号化鍵１３０７の共有履歴を用いた場合には、一度課金された後は何度もコンテンツの配信を可能とする定額サービスを実現することができる。また、シンボリックリンク等を用いてコンテンツ所在情報に一定の有効期間をもたせることで、その有効期間内であれば何度もコンテンツの配信を可能とする期間限定の定額サービスを実現することもできる。一方、コンテンツの配信履歴を用いた場合

には、配信する毎に課金する所謂ペイパービュー（Pay per View）のサービスを実現することができる。

【００４５】

図３は、第１実施例に係るコンテンツ受信端末１１００の構成例を示す図である。端末認証部１１０１は、コンテンツの配信を受ける際、ユーザの操作に応じて著作権保護システム１３００内の端末認証部１３０２に対し、認証に必要な情報（例えばコンテンツ受信端末１１００又は該コンテンツ受信端末１１００のユーザに付与されたＩＤとパスワード等）を送信することにより、該端末認証１３０２とともに認証処理を行う。

【００４６】

このような認証の後、著作権保護システム１３００内のコンテンツ選択文書配信部１３０４からコンテンツ選択文書１４００が送信される。コンテンツ選択文書受信部１１０２は、このコンテンツ選択文書１４００を受信する。コンテンツ選択文書検証部１１０８は、コンテンツ選択文書１４００に含まれている署名を検証することにより、該コンテンツ選択文書１４００の正当性を検証する。正当性が検証できた場合には、コンテンツ選択文書検証部１１０８は、このコンテンツ選択文書１４００をコンテンツ選択メニュー表示部１１１０へ出力する。コンテンツ選択メニュー表示部１１１０は、入力されたコンテンツ選択文書１４００に基づいて、コンテンツ受信端末１１００のユーザがコンテンツを選択するための画面（コンテンツ選択画面）を表示する。

【００４７】

コンテンツ受信端末１１００のユーザは、コンテンツ選択画面で配信を受けたいコンテンツを選択する。選択結果は、ユーザ選択受信部１１１１で受信される。所在情報暗号化復号部１１１２は、ユーザによって選択されたコンテンツに対応するコンテンツ所在情報及び所在認証情報を、受信したコンテンツ選択文書１４００から抽出する。所在情報暗号化復号部１１１２は、コンテンツ選択文書１４００に含まれる暗号化情報タグにより抽出したコンテンツ所在情報及び所在認証情報が暗号化されているか否かを判定し、暗号化されている場合には、所在情報暗号化鍵共有部１１０３において著作権保護システム１３００との間で共有さ

れている鍵１１０７を用いて、その暗号化されたコンテンツ所在情報及び所在認証情報を復号する。

【００４８】

コンテンツ配信サーバ検証部１１１３は、受信したコンテンツ選択文書１４００から、所在認証情報タグに基づいて、所在認証情報を抽出する。次に、コンテンツ配信サーバ検証部１１１３は、この所在認証情報に基づいてコンテンツの所在の正当性、換言すればコンテンツ配信サーバの正当性を判定する。コンテンツ配信サーバ検証部１１１３は、コンテンツ配信サーバが正当であると判定した場合にのみ、コンテンツ配信要求部１１０４へコンテンツ所在情報を出力する。コンテンツ配信要求部１１０４は、このコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対し、コンテンツの配信要求を送信する。

【００４９】

この配信要求に応じてコンテンツ配信サーバからコンテンツが配信されると、コンテンツ受信部１１０５は、このコンテンツを受信する。コンテンツ復号部１１１４は、コンテンツを構成する符号化された音楽データや映像データを復号し、それぞれの出力デバイス（図示せず）へ音声信号や映像信号を出力する。なお、受信したコンテンツが暗号化されている場合には、コンテンツ暗号化復号部１１０９は、その暗号化されたコンテンツを、コンテンツ暗号化鍵共有部１１０６によってコンテンツ配信サーバとの間で共有されている鍵を用いて復号し、コンテンツ復号部１１１４へ出力する。

【００５０】

上述した端末認証部１１０１、所在情報暗号化鍵共有部１１０３、コンテンツ配信要求部１１０４、コンテンツ暗号化鍵共有部１１０６、コンテンツ暗号化復号部１１０９、所在情報暗号化復号部１１１２、コンテンツ配信サーバ検証部１１１３及びコンテンツ復号部１１１４は、耐タンパー性を有するソフトウェア又はハードウェアで実装することにより、ユーザの不正操作を防止することができる。また、コンテンツ所在情報は、この耐タンパー性により、コンテンツ受信端末１１００のユーザを含め、外部への漏洩が防止される。

【００５１】

このように、本実施例のコンテンツ配信システム１０００では、著作権保護システム１３００は、暗号化部１３０９がコンテンツ所在情報及び所在認証情報を暗号化し、コンテンツ文書生成部１３１０が暗号化されたコンテンツ所在情報及び所在認証情報を複数組み合わせたコンテンツ選択文書を生成し、コンテンツ選択文書配信部１３０４が生成されたコンテンツ選択文書をコンテンツ受信端末１１００へ送信する。一方、コンテンツ受信端末１１００は、コンテンツ選択文書受信部１１０２が著作権保護システム１３００からのコンテンツ選択文書を受信し、所在情報暗号化復号部１１１２が受信したコンテンツ選択文書から暗号化されたコンテンツ所在情報を抽出して復号し、コンテンツ配信サーバ検証部１１１３が受信したコンテンツ選択文書から所在認証情報を抽出してコンテンツの所在の正当性を検証し、コンテンツ配信要求部１１０４が検証によりコンテンツの所在の正当性が確認された場合にコンテンツの配信要求を送出し、コンテンツ受信部１１０６がこの配信要求に応じてコンテンツサーバから配信されるコンテンツを受信する。

【００５２】

従って、コンテンツ配信サーバと著作権保護システム１３００が分離され、且つ、コンテンツの配信に際してコンテンツ配信サーバと著作権保護システム１３００との間で情報のやり取りが行われることがないため、コンテンツ配信サーバの負荷を軽減させて、大規模なコンテンツ配信システムを構築することができる。

【００５３】

また、従来のようにコンテンツ選択文書全体が暗号化されるのではなく、コンテンツ所在情報だけを選択的に暗号化されるため、課金種別に応じて暗号化された複数のコンテンツ所在情報をコンテンツ選択文書に含ませておくことで、効率的なコンテンツ課金を行うことができる。

【００５４】

更に、コンテンツ所在情報を暗号化することにより、第三者がコンテンツを利用することを防止することができるため、従来のように、コンテンツ配信サーバにおいて必ずしもコンテンツを暗号化する必要はない。このため、コンテンツ受

信端末１１００は、暗号化されたコンテンツの復号処理を省略することができ、演算量の軽減を図ることが可能となる。

【００５５】

また、著作権保護システム１３００からコンテンツ受信端末１１００へコンテンツの所在の正当性を証明する所在認証情報とが送信されるため、コンテンツ受信端末１１００は、コンテンツ所在情報で示されるコンテンツの所在の正当性を検証することができ、不正なサーバへアクセスして配信を受けることが防止され適切な課金処理を行うことができる。

【００５６】

図４は、本発明の第２実施例に係るコンテンツ配信システムの構成例を示す図である。同図に示す同図に示すコンテンツ配信システム２０００は、コンテンツ受信端末２１００と、著作権保護システムとコンテンツ配信サーバとが同一のサーバに実装された著作権保護システム兼コンテンツ配信サーバ２２００とを備えて構成される。コンテンツ受信端末２１００と、著作権保護システム兼コンテンツ配信サーバ２２００とは、ネットワーク２４００を介して接続される。

【００５７】

著作権保護システム兼コンテンツ配信サーバ２２００は、図１に示した第１実施例における著作権保護システム１３００と同様、オーディオビジュアルデータであるコンテンツの所在を示すコンテンツ所在情報を暗号化し、この暗号化されたコンテンツ所在情報、コンテンツの所在の正当性を証明する所在認証情報、及び送信元である著作権保護システム兼コンテンツ配信サーバ２２００の正当性を証明する署名を含んだコンテンツ選択文書２３００を生成し、コンテンツ受信端末２１００へ配信する。

【００５８】

コンテンツ受信端末２１００は、図１に示した第１実施例におけるコンテンツ受信端末１１００と同様、受信したコンテンツ選択文書２３００に含まれている署名の検証、ユーザが選択したコンテンツに対応するコンテンツ所在情報の復号、コンテンツの所在の正当性の判定を行った上で、コンテンツ所在情報で指定されるコンテンツの配信要求を著作権保護システム兼コンテンツ配信サーバ２２０

０へ送信し、この配信要求に応じて配信されるコンテンツを受信する。

【００５９】

このように、著作権保護システムとコンテンツ配信サーバとが同一のサーバに実装されるようにしても良い。この場合、コンテンツ所在情報は、サーバ内のアドレス情報又はディレクトリ情報となる。

【００６０】

図５は、本発明の第３実施例に係るコンテンツ配信システムの構成例を示す図である。同図に示す同図に示すコンテンツ配信システム３０００は、コンテンツ受信端末３１００、著作権保護システム３２００、コンテンツサーバ群３４００、コンテンツホルダ３６００を備えて構成される。コンテンツ受信端末２１００と、著作権保護システム３２００及びコンテンツ配信サーバ３４００とは、ネットワーク３５００を介して接続される。

【００６１】

コンテンツホルダ３６００は、オーディオビジュアルデータであるコンテンツの所在を示すコンテンツ所在情報や該コンテンツに関連するアクセス制御情報（課金情報等）を含んだコンテンツ選択文書３７００を生成し、著作権保護システム３２００へ送信する。

【００６２】

著作権保護システム３２００は、受信したコンテンツ選択文書３７００をコンテンツ受信端末３１００へ送信するためのコンテンツ選択文書３３００に変換する。この際、著作権保護システム３２００は、コンテンツの所在の正当性を証明する所在認証情報の付与、アクセス情報に基づくコンテンツ所在情報の暗号化、コンテンツ選択文書の送信元となる著作権保護システム３２００の正当性を証明する署名を付与する。なお、コンテンツホルダ、コンテンツサーバ運営者が所在認証情報を発行するようにしても良い。

【００６３】

コンテンツ受信端末３１００は、図１に示した第１実施例におけるコンテンツ受信端末３１００と同様、受信したコンテンツ選択文書３３００に含まれている署名の検証、ユーザが選択したコンテンツに対応するコンテンツ所在情報の復号

、コンテンツの所在の正当性の判定を行った上で、コンテンツ所在情報で指定されるコンテンツの配信要求をコンテンツ配信サーバへ送信し、この配信要求に応じて配信されるコンテンツを受信する。

【００６４】

なお、上述した第１乃至第３の実施例では、著作権保護システムはコンテンツ所在情報及び所在認証情報の双方を暗号化したが、コンテンツ所在情報のみを暗号化しても良い。

【００６５】

ところで、上述したように、コンテンツ選択文書にはコンテンツの所在の正当性を証明する所在認証情報や暗号化されたコンテンツ所在情報を埋め込む必要がある。これら所在認証情報や暗号化されたコンテンツ所在情報の埋め込みには、インターネット上で交換されるデータの記述言語として一般的になりつつあるＸＭＬ（eXtensible Makeup Language）を利用することができる。

【００６６】

ＸＭＬは、ユーザがタグを自由に定義することができる汎用的なデータ記述言語であり、所在認証情報であることを示すタグ（所在認証情報タグ）やコンテンツ所在情報が暗号化されていることを示すタグ（暗号化情報タグ）をも定義することができる。また、Ｗ３Ｃでは、文書の一部分に対する署名を実現することができるＸＭＬ－ｓｉｇｎａｔｕｒｅの標準化が進められている。このＸＭＬ－ｓｉｇｎａｔｕｒｅは、署名に関する情報をタグ付けし、ＸＭＬ文書で表すための規格であり、ｈｔｍｌやＸＭＬの文書の中にテキスト形式で署名情報を埋め込むことを可能にしている。このため、所在認証情報や暗号化されたコンテンツ所在情報の埋め込みにＸＭＬを利用することが可能となる。

【００６７】

図６は、ＸＭＬ－ｓｉｇｎａｔｕｒｅの構造を示す図である。同図に示すようにＸＭＬ－ｓｉｇｎａｔｕｒｅはＳｉｇｎａｔｕｒｅエレメント４０００で始まる。このＳｉｇｎａｔｕｒｅエレメント４０００は、ＳｉｇｎｅｄＩｎｆｏエレメント４１００、Ｓｉｇｎａｔｕｒｅ　Ｖａｌｕｅエレメント４２００、ＫｅｙＩｎｆｏエレメント４３００からなる。ここで、ＳｉｇｎｅｄＩｎｆｏエレメン

ト４１００には、署名に用いられるアルゴリズム、個々の署名対象のＵＲＩ、署名対象のハッシュ値が含まれる。Ｓｉｇｎａｔｕｒｅ　Ｖａｌｕｅエレメント４２００は、ＳｉｇｎｅｄＩｎｆｏエレメント４１００についての署名値であり、ＳｉｇｎｅｄＩｎｆｏエレメント４１００が改竄されていないことを証明する。ＫｅｙＩｎｆｏエレメント４３００は、署名値を検証するための鍵データである。

【００６８】

コンテンツの所在の正当性を証明する所在認証情報の埋め込みにＸＭＬ－ｓｉｇｎａｔｕｒｅを利用する場合、認証局又は著作権保護システムで生成されたコンテンツ配信サーバに対する証明情報のＵＲＩをＲｅｆｅｒｅｎｃｅエレメント４１３０に、この証明情報から生成される認証情報をＳｉｇｎａｔｕｒｅ　Ｖａｌｕｅエレメント４２００にそれぞれ埋め込む。また、認証情報を生成するために使用したアルゴリズムをＳｉｇｎｅｄＩｎｆｏエレメント４１００に、認証情報を検証するための鍵とその鍵の共有方法とをＫｅｙＩｎｆｏエレメント４３００にそれぞれ埋め込む。

【００６９】

また、暗号化されたコンテンツ所在情報をコンテンツ選択文書に埋め込む場合には、ＩＢＭ東京基礎研究所の村山氏らが提案するＥｌｅｍｅｎｔ－Ｗｉｓｅ　ＸＭＬ　Ｅｎｃｒｙｐｔｉｏｎ（http://lists.w3.org/Archives/Public/xml-encryption/2000Apr/att-0005/01-xmlenc 参照）等を利用することができる。本提案は、ＸＭＬ文書のエレメント単位で暗号化を施すことを可能にするものであり、図７に示すように、暗号化エレメント内に暗号文と暗号化に用いたアルゴリズムとを埋め込むことができる。

【００７０】

上記各例において、著作権保護システム１３００内の暗号化部１３０９が暗号化手段に、コンテンツ文書生成部１３１０がコンテンツ選択文書生成手段に、コンテンツ選択文書配信部１３０４がコンテンツ選択文書送信手段に対応する。また、コンテンツ受信端末１１００内のコンテンツ選択文書受信部１１０２がコンテンツ選択文書受信手段に、所在情報暗号化復号部１１１２がコンテンツ所在情

報を抽出手段及び復号手段に、コンテンツ配信サーバ検証部１１１３が所在認証情報抽出手段及び正当性検証手段に、コンテンツ配信要求部１１０４が配信要求送出手段に、コンテンツ受信部１１０６がコンテンツ受信手段に対応する。

【００７１】

【発明の効果】

上述の如く、本願発明によれば、コンテンツ配信サーバと著作権保護システムが分離され、且つ、コンテンツの配信に際してコンテンツ配信サーバと著作権保護システムとの間で情報のやり取りが行われることがないため、コンテンツ配信サーバの負荷を軽減させて、大規模なコンテンツ配信システムを構築することができる。

【００７２】

また、従来のようにコンテンツ選択文書全体が暗号化されるのではなく、コンテンツ所在情報だけを選択的に暗号化することが可能であるため、例えば課金種別に応じて暗号化された複数のコンテンツ所在情報をコンテンツ選択文書に含ませておくことで、効率的なコンテンツ課金を行うことができる。

【００７３】

また、著作権保護システムからコンテンツ受信端末へコンテンツの所在の正当性を証明する所在認証情報が送信されるため、コンテンツ受信端末は、コンテンツ所在情報で示されるコンテンツの所在の正当性を検証することができ、不正なサーバへアクセスして配信を受けることが防止され適切な課金処理を行うことができる。

【００７４】

特に、コンテンツ選択文書に課金種別等のコンテンツへのアクセス制御情報を付与することで、著作権保護システムがコンテンツ所在情報に対する暗号化を適切に行うことが可能になる。

【図面の簡単な説明】

【図１】

第１実施例に係るコンテンツ配信システムの構成例を示す図である。

【図２】

第１実施例に係る著作権保護システムの構成例を示す図である。

【図３】

第１実施例に係るコンテンツ受信端末の構成例を示す図である。

【図４】

第２実施例に係るコンテンツ配信システムの構成例を示す図である。

【図５】

第３実施例に係るコンテンツ配信システムの構成例を示す図である。

【図６】

ＸＭＬ－Ｓｉｇｎａｔｕｒｅの構造を示す図である。

【図７】

Ｅｌｅｍｅｎｔ－Ｗｉｓｅ　ＸＭＬ　Ｅｎｃｒｙｐｔｉｏｎの手順を示す図である。

【図８】

コンテンツ配信サーバが認証、課金を行わない場合の従来のコンテンツ配信システムの構成例を示す図である。

【符号の説明】

１０００　コンテンツ配信システム

１１００　コンテンツ受信端末

１１０１　端末認証部

１１０２　コンテンツ選択文書受信部

１１０３　所在情報暗号化鍵共有部

１１０４　コンテンツ配信要求部

１１０５　コンテンツ受信部

１１０６　コンテンツ暗号化鍵共有部

１１０７　鍵

１１０８　コンテンツ選択文書検証部

１１０９　コンテンツ暗号化復号部

１１１０　コンテンツ選択メニュー表示部

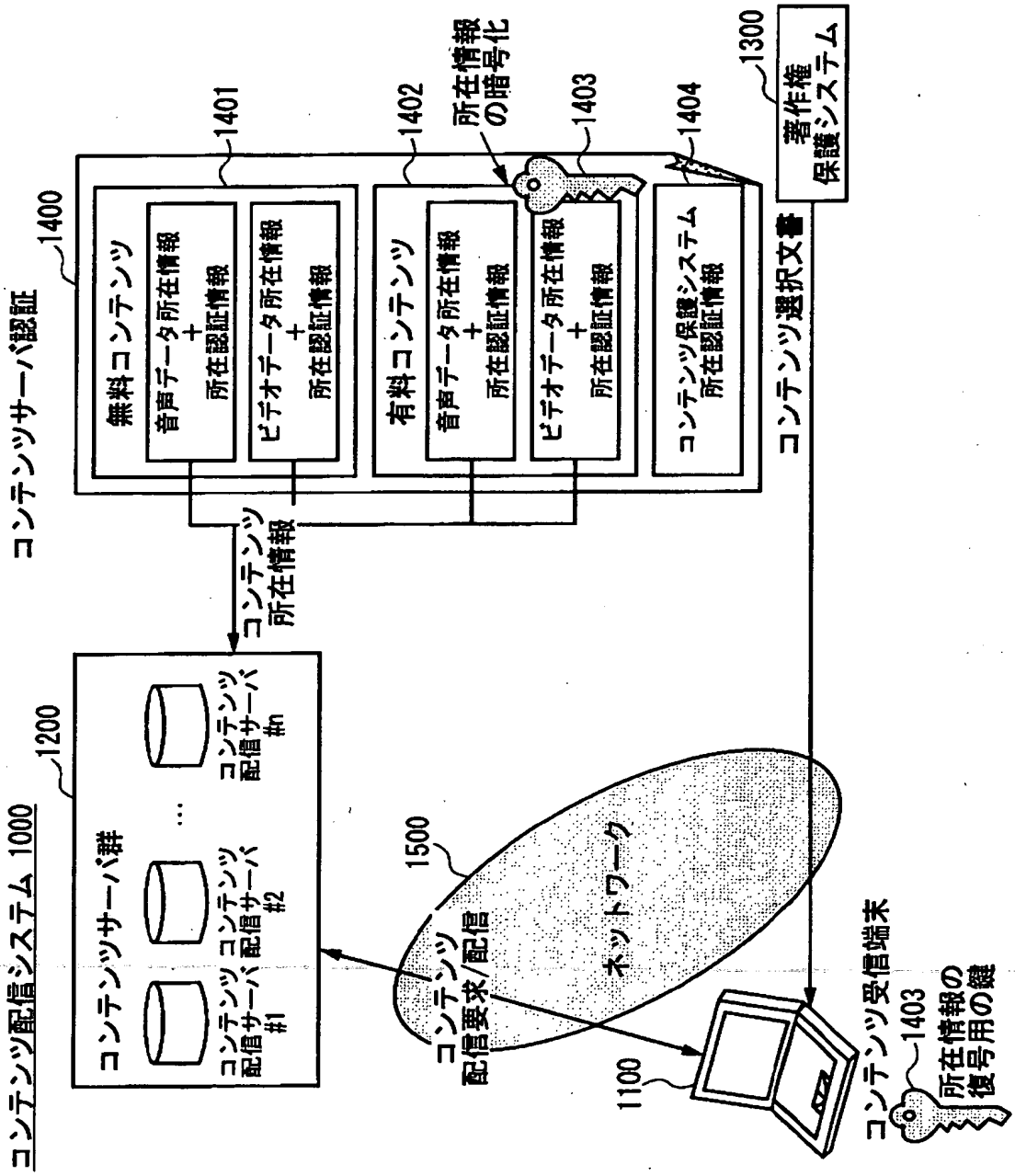
１１１１　ユーザ選択受信部

１１１２　所在情報暗号化復号部
１１１３　コンテンツ配信サーバ検証部
１１１４　コンテンツ復号部
１２００　コンテンツサーバ群
１３００　著作権保護システム
１３０１　アクセス情報受信部
１３０２　端末認証部
１３０３　所在情報暗号化鍵共有部
１３０４　コンテンツ選択文書受信部
１３０５　課金情報蓄積サーバ
１３０６　課金部
１３０７　鍵
１３０８　コンテンツ所在情報
１３０９　暗号化部
１３１０　コンテンツ選択文書生成部
１３１１　所在認証情報
１３１２　所在認証情報タグ付加部
１３１３　署名部
１３１４　情報付加部
１４００　コンテンツ選択文書
１５００　ネットワーク

【書類名】　図面

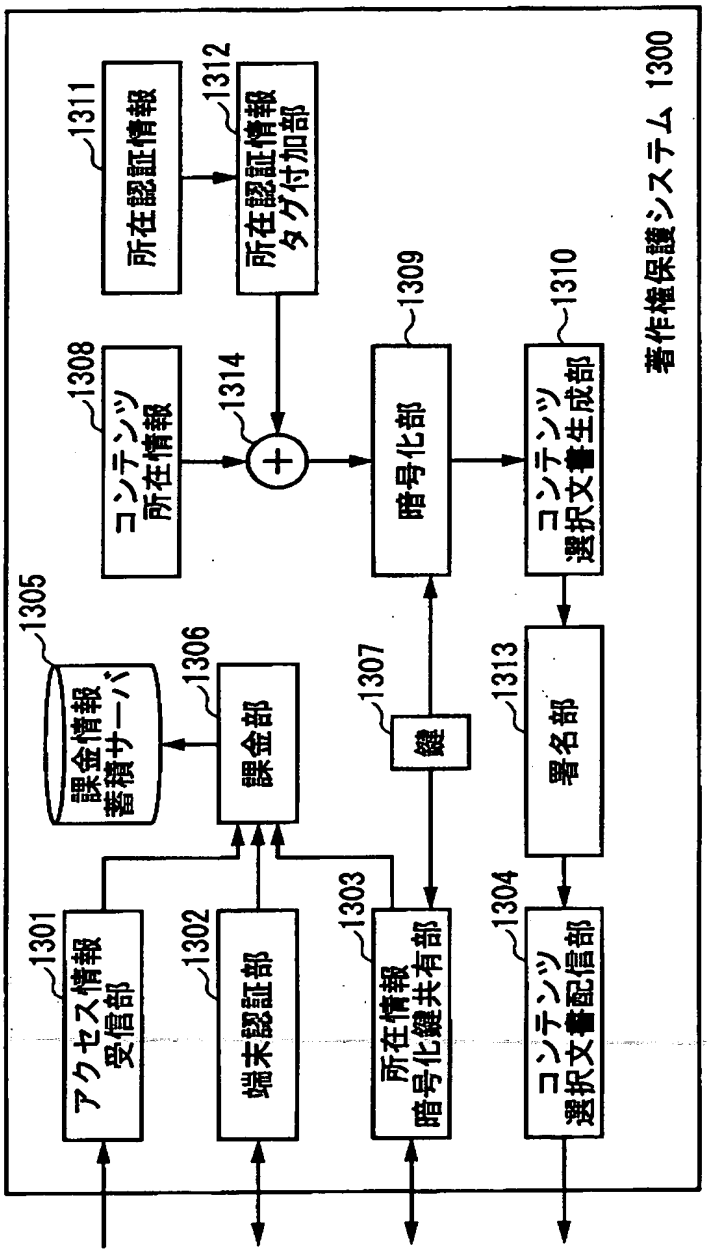
【図１】

第１実施例に係るコンテンツ配信システムの構成例を示す図



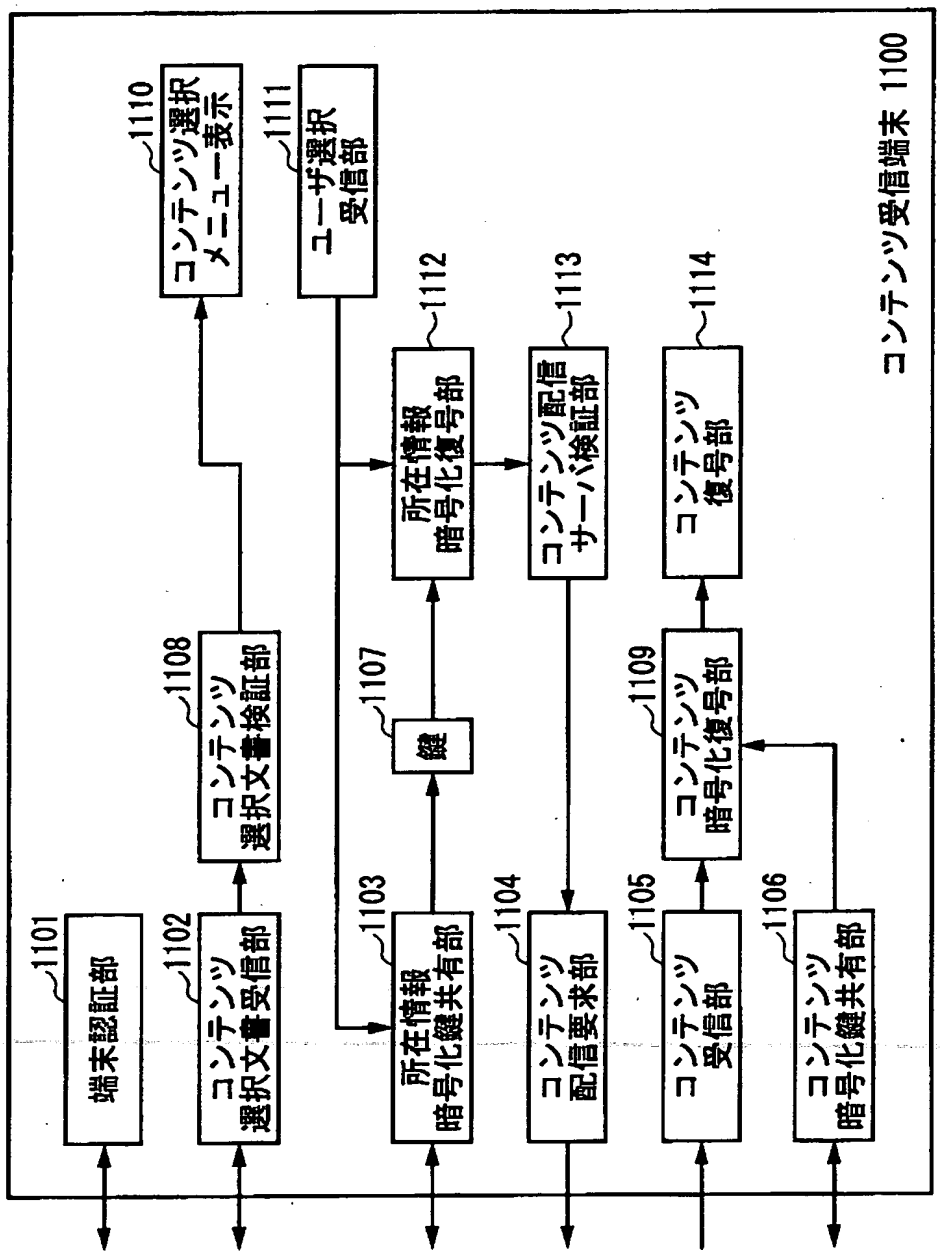
【図２】

第１実施例に係る著作権保護システムの構成例を示す図



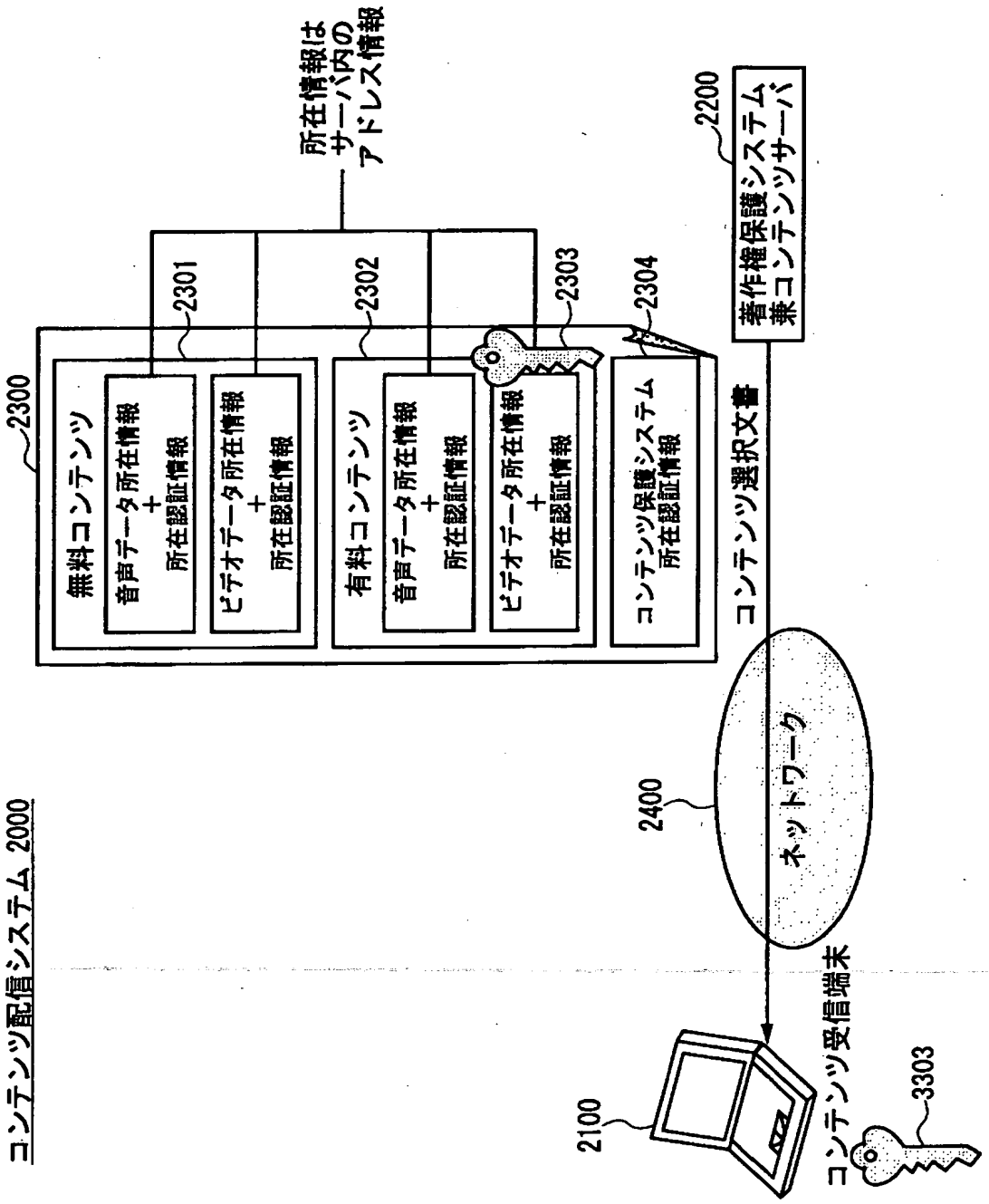
【図３】

第１実施例に係るコンテンツ受信端末の構成例を示す図



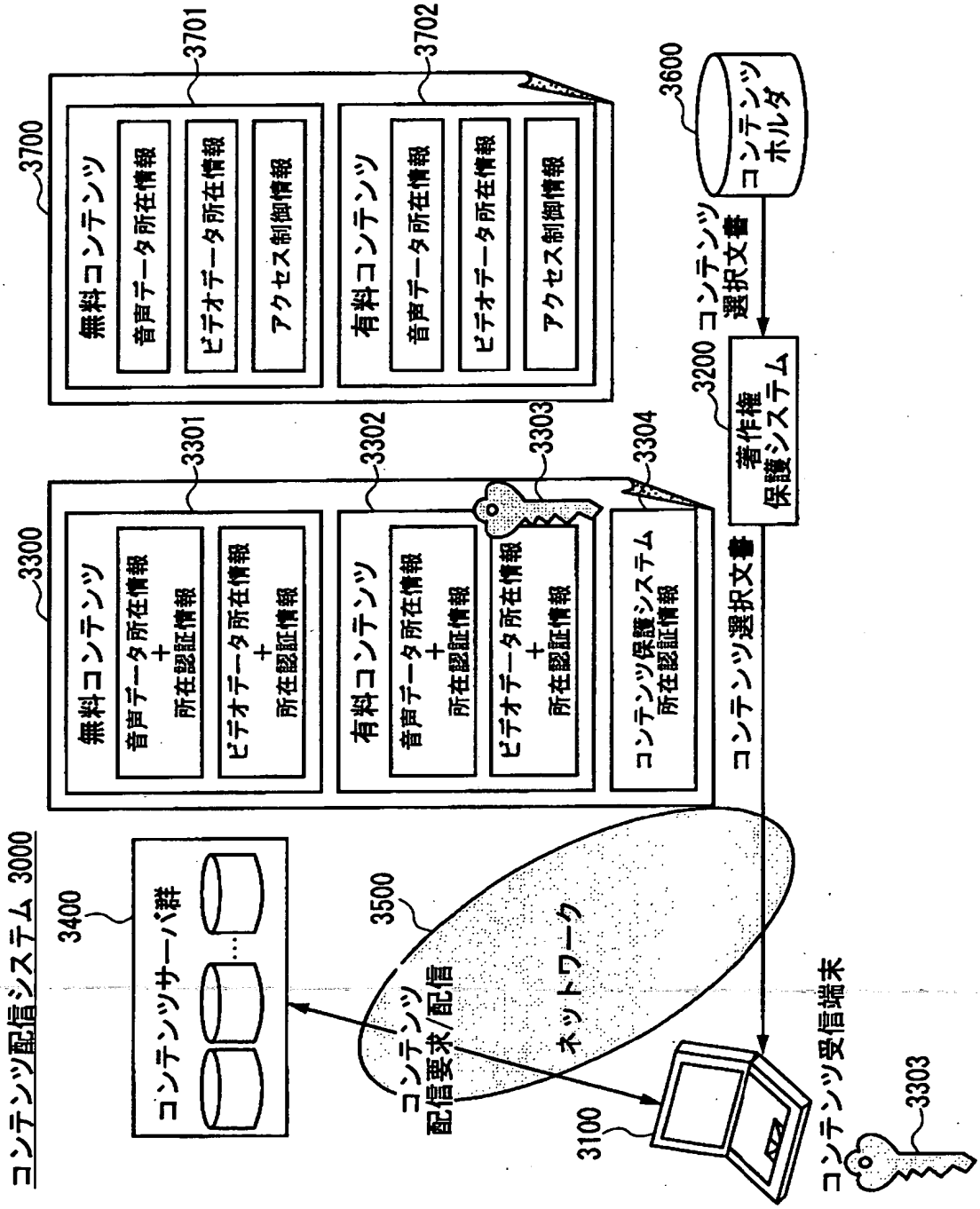
【図４】

第２実施例に係るコンテンツ配信システムの構成例を示す図



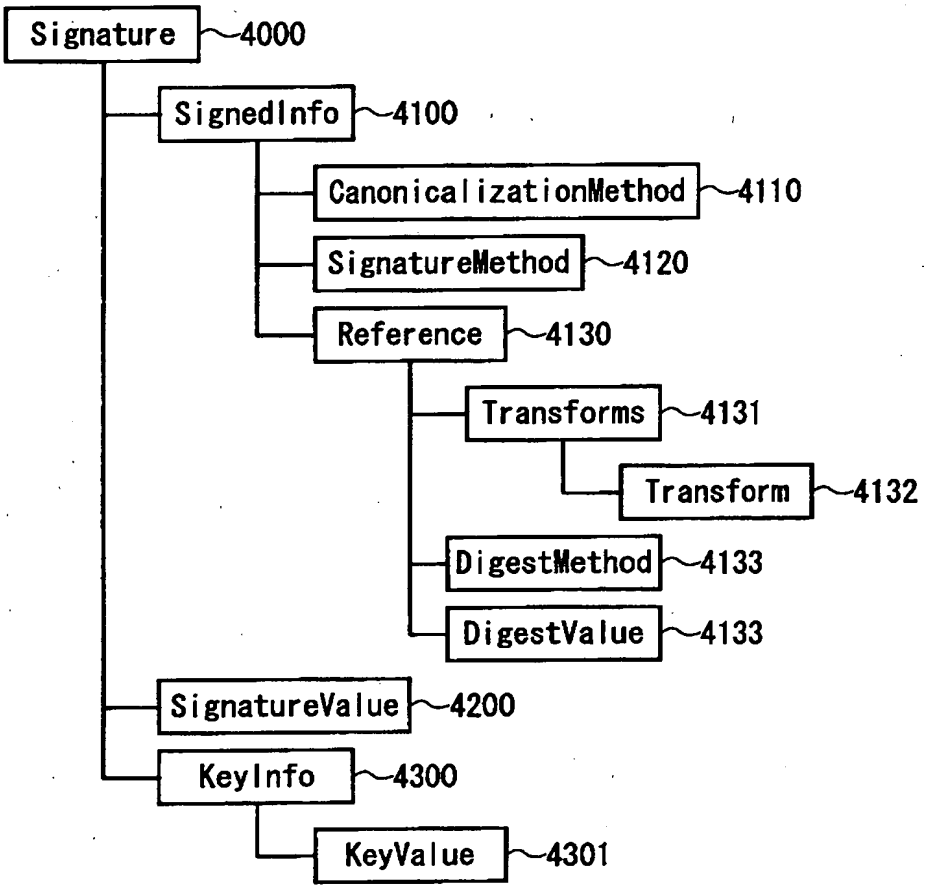
【図５】

第３実施例に係るコンテンツ配信システムの構成例を示す図



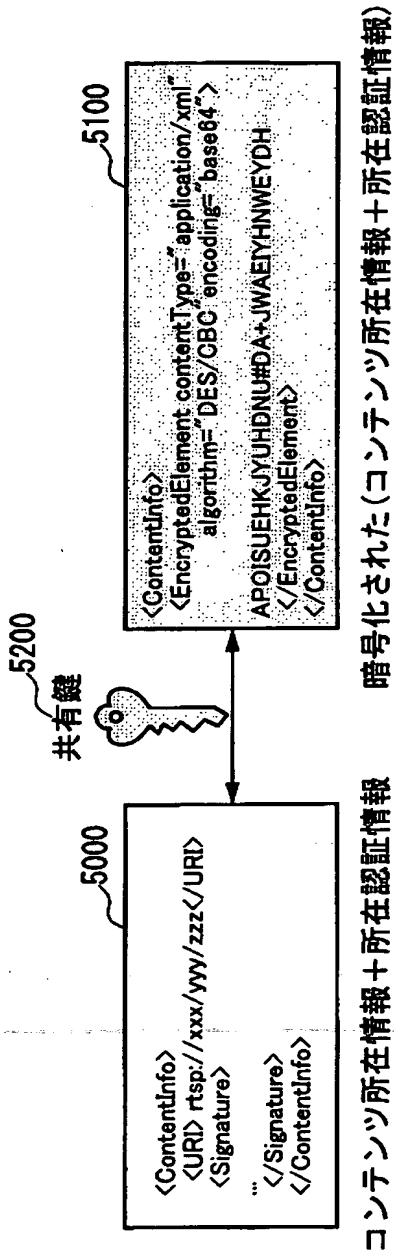
【図６】

ＸＭＬ－Ｓｉｇｎａｔｕｒｅの構造を示す図



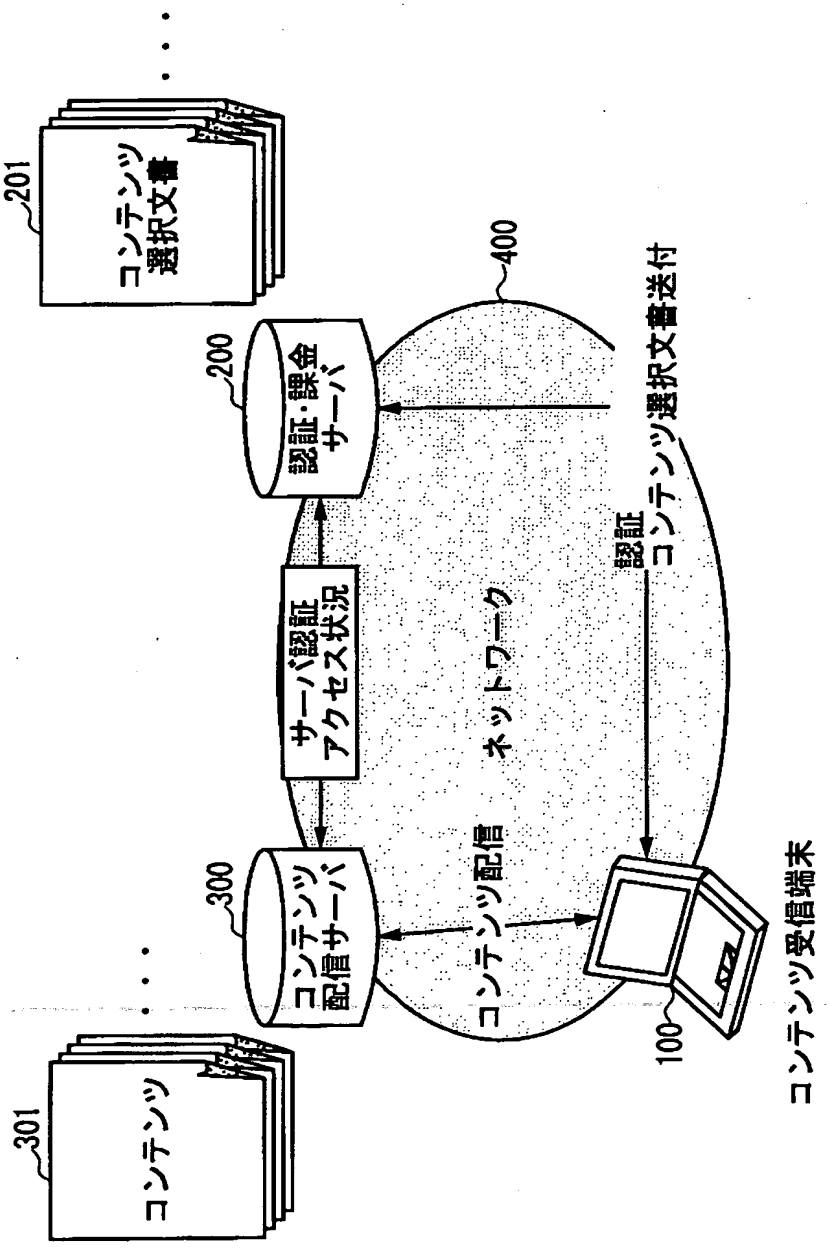
【図７】

Ｅｌｅｍｅｎｔ-Ｗｉｓｅ ＸＭＬ Ｅｎｃｒｙｐｔｉｏｎの手順を示す図



【図８】

コンテンツ配信サーバが認証、課金を行わない場合の
従来のコンテンツ配信システムの構成例を示す図



【書類名】　　要約書

【要約】

【課題】　大規模なシステムを構築可能であるとともに、コンテンツ課金を適正に行うことができるコンテンツ配信システム、著作権保護システム及びコンテンツ受信端末を提供する。

【解決手段】　著作権保護システム１３００は、所在認証情報が付加されたコンテンツ所在情報を暗号化し、この暗号化したコンテンツ所在情報と所在認証情報とを含んだコンテンツ選択文書を生成してコンテンツ受信端末１１００へ送信する。コンテンツ受信端末１１００は、このコンテンツ選択文書を受信し、暗号化されたコンテンツ所在情報及び所在認証情報を抽出して復号し、所在認証情報によりコンテンツの所在の正当性を検証し、コンテンツの所在の正当性が確認された場合にコンテンツ所在情報で指定されるコンテンツ配信サーバに対し配信要求を送出し、この配信要求に応じて配信されるコンテンツを受信する。

【選択図】　　図１

# 出　願　人　履　歴　情　報

識別番号　　〔３９２０２６６９３〕

１．変更年月日　　２０００年　５月１９日
［変更理由］　名称変更
住　所　　東京都千代田区永田町二丁目１１番１号
氏　名　　株式会社エヌ・ティ・ティ・ドコモ